$\mathbb{Q}(^3\sqrt{m})$の類群の3-Rankを計算するアルゴリズム (代数的整数論)

AUTHOR(S):

小林, 新樹

CITATION:

小林, 新樹. $\mathbb{Q}(^3\sqrt{m})$の類群の3-Rankを計算するアルゴリズム (代数的整数論). 数理解析研究所講究録 1975, 230: 41-46

ISSUE DATE:

1975-03

URL:

http://hdl.handle.net/2433/105436

数理解析研究所講究録
230巻 1975年 41-46

$\mathbb{Q}(\sqrt[3]{m})$ の類群の 3-rank を計算するアルゴリズム

都立大理　　小林新樹

以下の結果は、東大紀要 21(1974), 263-270 に出ているので詳しくは、そちらを見て頂きたい。

k を有限次代数体、C_k をその ideal 類群とするとき、

$$d^{(3)}C_k = \dim_{\mathbb{F}_3}(C_k/C_k^3)$$

とおく。目標は、立方因子を含まない有理整数 m に対して

$$\Omega = \mathbb{Q}(\sqrt[3]{m})$$

としたとき、$d^{(3)}C_\Omega$ を計算するためのアルゴリズムを求めることで、m が $p \not\equiv \pm 1 \pmod 9$ なる 3 以外の素因子 p を少くも 1 個含めば、実際に実行できるものである。

I　$k=\mathbb{Q}(\sqrt{-3})$, $K=k(\sqrt[3]{m})$ とし、$\tilde{\Omega}$, $\tilde{K}$ をそれぞれ、C_Ω^3 および C_K^3 に対応する Ω および K 上の類体とする。その時、次数の関係から、$d^{(3)}C_\Omega = [\tilde{\Omega}:\Omega] = [\tilde{\Omega}K:K]$ で、$G(\tilde{K}/\tilde{\Omega}K)$ は $G(\tilde{K}/\Omega)$ の交換子群であることがわかるから、それを計算すれ

ばよい。ところで τ を複素共役とすれば、τ は $\rho \mapsto \tau\rho\tau^{-1}$ によって $G(\tilde{K}/K)$ 上に作用し、これに関して $G(\tilde{K}/\Omega) = G(\tilde{K}/K)\cdot\langle\tau\rangle$（半直積）となっている。更に $G(\tilde{K}/K)$ は $\mathbb{F}_3$ 上の線型空間になっているので、次のことがわかる。

$G(\tilde{K}/K)$ の勝手な基底に関する τ の作用の表現を X とすれば、$d^{(3)}C_\Omega$ は、X の固有値の中で、1 の重複度に等しい。

Ⅱ　よって問題は、$G(\tilde{K}/K)$ の適当な基底を見つけることに帰着される。

①　$G(K/k) = \langle\sigma\rangle$ としたとき、$C_K^{1-\sigma}$ に対応する K 上の類体を K_1 とおけば、$K_1 \subset \tilde{K}$ で、$G(\tilde{K}/K_1)$ は $G(\tilde{K}/K)$ の τ-不変な部分空間である。従って、上述の 1 の重複度は、$G(\tilde{K}/K_1)$ 上、および $G(\tilde{K}/K)/G(\tilde{K}/K_1) = G(K_1/K)$ 上のそれらの和となる。ここで $G(K_1/K)$ 上の重複度は、Ⅰにおけると同様の意味で、Fröhlich の意味での、Ω 上の genus field に対応して、

$$\#\{p \mid m \mid p \equiv 1 \pmod 3\}$$

に等しいことが知られている。

②　残るのは $G(\tilde{K}/K_1)$ 上での τ の表現である。そのために、次の2つの事実に注意する。

(1)　$G(\tilde{K}/K_1)$ は $G(\tilde{K}/k)$ の交換子群であって、その中

心に含まれる。従って $[x, y]$ は $G(\tilde{K}/k)$ の上で bilin. で その値は $G(\tilde{K}/k)/G(\tilde{K}/K_1) = G(K_1/k)$ における x, y の剰余類にしかよらない。

(12). $\mathfrak{f} = \mathfrak{f}(K/k)$ (導手) の各素因子 $\mathfrak{p}$ に対して $G(K_1/k)$ におけるその惰性群の生成元を $\sigma_{\mathfrak{p}}$ とし、それの $\tilde{K}$ への延長をも同じ文字で表わすことにする。そのとき、$G(\tilde{K}/k)$ は $\{\sigma_{\mathfrak{p}} \mid \mathfrak{p} \mid \mathfrak{f}\}$ で、$G(\tilde{K}/K_1)$ は $\{[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}] \mid \mathfrak{p}, \mathfrak{q} \mid \mathfrak{f}\}$ で 生成される。

特に(1)によれば、$\tau[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}]\tau^{-1}$ を知るためには、$\tau\sigma_{\mathfrak{p}}\tau^{-1}$ 等を $G(K_1/k)$ の中で知ればよいことがわかる。あとで見るように、常に $\tau\sigma_{\mathfrak{p}}\tau^{-1} = \sigma_{\tau\mathfrak{p}}{}^{-1}$ となるように $\sigma_{\mathfrak{p}}$ を選ぶことができるから、結局、$[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}]$ の形の元の間の一次関係をすべて求めることができればよいわけである。

III 上の(1), (12) は Kummer 拡大 K/k の生成元が有理数であることには依存していないので、以下、

$$K = k(\sqrt[3]{\alpha}), \qquad \alpha \in k^{\times}$$

として考える。$\mathfrak{f} = \mathfrak{f}(K/k)$ の素因子を $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ とし、$\sigma_i = \sigma_{\mathfrak{p}_i} \in G(\tilde{K}/k)$ を(12)のようにとる。$\zeta = \zeta_3$ (1の原始3乗根)を1つ固定したとき、$\sigma_i \sqrt[3]{\alpha} = \zeta\sqrt[3]{\alpha}$ であるとしてよく、特に、

$$(*) \qquad \prod_{i=1}^{t} \sigma_i^{a_i} \in G(\tilde{K}/K) \iff \sum_{i=1}^{t} a_i \equiv 0 \pmod 3$$

が成立つ。従ってまた $[\sigma_i, \sigma_j] = [\sigma_i, \sigma_k][\sigma_k, \sigma_j]$ となる。結局 $\{[\sigma_1, \sigma_i] \mid i = 2, \cdots, t\}$ の間の一次関係を求めればよい。

III a. $[x, y]$ の bilinearity によって、

$$\prod_{i=2}^{t} [\sigma_1, \sigma_i]^{a_i} = [\sigma_1, \sigma_1^{-a_1} \prod_{i=2}^{t} \sigma_i^{a_i}], \quad a_1 = -\sum_{i=2}^{t} a_i$$

となるが、上の (*) によって $\sigma_1^{-a_1} \prod \sigma_i^{a_i} \in G(\tilde{K}/K)$, 従って

$$\sigma_1^{-a_1} \prod \sigma_i^{a_i} = \left(\frac{\tilde{K}/K}{c}\right), \ {}^{\exists} c \in C_K,$$

と書ける。ここで $\tilde{K}$ は $C_K^3 = C_K^{(1-\sigma_1)^2}$ に対応しているので、上の交換子を計算して、

$$\prod_{i=2}^{t} [\sigma_1, \sigma_i]^{a_i} = 1 \iff c \in C_K^{1-\sigma_1} C_K^G.$$

ここで、$\mathfrak{p}_i$ の K における因子を $\mathfrak{P}_i$ とすれば、C_K^G は $\mathfrak{P}_1, \cdots, \mathfrak{P}_t$ で生成されるか。そうでなければ、あと1つ class を追加すればよく、そのときは、追加すべき class より1つ ideal をとって $\mathfrak{P}_{t+1}$ とおき、$\mathfrak{p}_{t+1} = N_{K/k}(\mathfrak{P}_{t+1})$ とおく。そうしたとき、上の $c \in C_K$ より1つ ideal $\mathfrak{A}$ をとれば、

$$c \in C_K^{1-\sigma_1} C_K^G \iff \mathfrak{A} = \mathfrak{a}^{1-\sigma_1} \prod_j \mathfrak{P}_j^{x_j}(\gamma), \ {}^{\exists}\mathfrak{a}: K\text{の ideal}, \ {}^{\exists}\gamma \in K^\times, \ {}^{\exists}(x_j).$$

$$\iff N_{K/k}(\mathfrak{A}) = \prod_j \mathfrak{p}_j^{x_j}(N_{K/k}(\gamma)), \ {}^{\exists}\gamma \in K^\times, \ {}^{\exists}(x_j).$$

$$\iff \beta = \zeta^w \prod_j \pi_j^{x_j} N_{K/k}(\gamma), \ {}^{\exists}\gamma \in K^\times, \ {}^{\exists}(w, x_j)$$

ここで、π_j, β は $\mathfrak{p}_j, N_{K/k}(\mathfrak{A})$ の k における勝手な生成元である。従って Hasse の norm 定理を使えば、

$$\prod_{i=2}^{t}[\sigma_1,\sigma_i]^{q_i}=1 \iff \left(\frac{\zeta,\alpha}{\mathfrak{p}}\right)^{w}\prod_j\left(\frac{\pi_j,\alpha}{\mathfrak{p}}\right)^{x_j}=\left(\frac{\beta,\alpha}{\mathfrak{p}}\right),\ \mathfrak{p}\text{ in }k$$

なる連立方程式が (w, x_j) なる解をもつ。

但し、実際は、両辺とも、$\mathfrak{p}$ 外なら 1 に等しく、方程式は $\mathfrak{p}$ 内 に対するものだけである。

III. あとは、各 $(a_2,\cdots,a_t)$ に対して $\left(\frac{\beta,\alpha}{\mathfrak{p}}\right)$ を求めればよい。まず

$$\sigma_1^{-a_1}\prod\sigma_i^{a_i}=\left(\frac{\tilde{K}/K}{\mathfrak{U}}\right)$$

となる K の ideal $\mathfrak{U}$ を探すのであるが、$[\sigma_1,*]=1$ を見るのであるから、II の (1) によって、この両辺が $G(K_1/k)$ で等しくなる。即ち

$$\sigma_1^{-a_1}\prod\sigma_i^{a_i}=\left(\frac{K_1/K}{\mathfrak{U}}\right)=\left(\frac{K_1/k}{N_{K/k}(\mathfrak{U})}\right)\quad \text{on } K_1$$

となる $\mathfrak{U}$ を探せばよい。今、$f_1=f(K_1/k)$ とおいたとき、$\beta_i\in k^\times$ を、

$$\beta_i\not\equiv 0\ (\mathfrak{p}_i),\quad \beta_i\equiv 1\ (\mathfrak{f}_1/\mathfrak{f}_1^{(\mathfrak{p}_i)}),\quad \left(\frac{\beta_i,\alpha}{\mathfrak{p}_i}\right)=\zeta.$$

なる元とすれば、$\left(\frac{\beta_i,K_1/k}{\mathfrak{p}_i}\right)$ は $G(K_1/k)$ における $\mathfrak{p}_i$ の惰性群の元で、

$$\left(\frac{\beta_i,K_1/k}{\mathfrak{p}_i}\right)\sqrt[3]{\alpha}=\zeta\sqrt[3]{\alpha}$$

となる。従って、$\left(\frac{\beta_i,K_1/k}{\mathfrak{p}_i}\right)=\left(\frac{K_1/k}{(\beta_i)}\right)$ は III の初めに選んだ σ_i に等しく、よって

$$\sigma_1^{-a_1}\prod\sigma_i^{a_i}=\left(\frac{K_1/k}{(\beta_1^{-a_1}\prod\beta_i^{a_i})}\right)\quad \text{on } K_1.$$

既に、上のような $\mathfrak{A}$ に対して

$$N_{K/k}(\mathfrak{A})\sim(\beta_1^{-a_1}\prod\beta_i^{a_i})\pmod{\mathfrak{f}_1}.$$

従って β を適当に選べば、

$$\beta\equiv\beta_1^{-a_1}\prod_{i=2}^{t}\beta_i^{a_i}\quad(\mathfrak{f}_1).$$

$\mathfrak{f}\mid\mathfrak{f}_1$ であるから、結局、各 $(a_2,\cdots,a_t)$ に対して、

$$\prod_{i=2}^{t}[\sigma_1,\sigma_i]^{a_i}=1$$

$$\Leftrightarrow\left(\frac{\zeta,\alpha}{\mathfrak{f}}\right)^{w}\prod_j\left(\frac{\pi_j,\alpha}{\mathfrak{f}}\right)^{x_j}=\begin{cases}\zeta^{-a_1}, & \mathfrak{f}=\mathfrak{f}_1,\ a_1=\sum_{i=2}^{t}a_i\\ \zeta^{a_i}, & \mathfrak{f}=\mathfrak{f}_2,\cdots,\mathfrak{f}_t\end{cases}$$

なる連立方程式が (w,x_j) について解をもつ。

また、$\alpha=m\in\mathbb{Z}$ のとき、$\tau\sigma_{\mathfrak{p}}\tau^{-1}=\sigma_{\tau\mathfrak{p}}^{-1}$ on K_1 となることも、上の σ_i の表現から明らかである。